Attorney Docket No: D02236-02 PATENT

UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| APPLICANT: | Alexander Medvinsky, et al. | GROUP ART UNIT: | 2135 |
| APPLN. NO.: | 09/890,180 | EXAMINER: | To, Baotran N. |
| FILED: | January 24, 2002 | Confirmation No.: | 7559 |
| TITLE: | **KEY MANAGEMENT FOR TELEPHONE CALLS TO PROTECT SIGNALING AND CALL PACKETS BETWEEN CTA'S** | | |

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## PRE-APPEAL BRIEF REQUEST FOR REVIEW

In response to the Final Office Action mailed from the U.S. Patent and Trademark Office on January 23, 2009, Applicants request review of the final rejection in the above-identified application. This request is being filed with a Notice of Appeal and required fee. An extension of time is requested and this response is accompanied by the fee required under 37 C.F.R. 1.136(a). The Commissioner is hereby authorized to charge any additional fees which may be required at any time during the prosecution of this application without specific authorization, or credit any overpayment, to Deposit Account No. 50-2117. No amendments are being filed with this request. The review is requested for the reasons stated in the remarks below.

## REMARKS

Claims 1-19 are pending in this application, and stand finally rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Barkan, European Patent Application Number 0 738 058 (hereinafter "Barkan"), in view of Ganesan, U.S. Patent Number 5,838,792 (hereinafter "Ganesan"). The Applicants respectfully traverse.

The Barkan reference describes an apparatus for transferring an encryption key in a secure way to facilitate establishing a secure communication link. The Barkan apparatus includes a key management device attached to each user's encryption machine. The key management device contains a list of secure communication partners and their

respective encryption keys and parameters. To initiate a secure link session, the user keys-in the identification of the desired addressee. If the details of the addressee are available, the Barkan apparatus automatically transfers the encryption key and the other communication parameters for the addressee to the encryption machine to establish the secure link. If the details of the addressee are not available, the Barkan apparatus automatically connects to a secure key distribution center to get the encryption key and parameters for that addressee. After establishing the secure link session between a first user's encryption machine and a second user's encryption machine, Barkan describes a communication path that is from the first user's encryption machine (element 21), through a communication channel (element 213) for the first user (facility 1), through a communication channel (element 233) for the second user (facility 3), and to the second user's encryption machine (element 23). Thus, the established secure link session in Barkan is a **direct communication path** from the first user's encryption machine to the second user's encryption machine.

The Office Action acknowledges that the Barkan reference does not describe generating a secret key at the first gateway controller; distributing the secret key to the first and second telephony adapters over previously established secure connections; and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key. To make up for these shortcomings, the Examiner relies on the Ganesan reference.

The Ganesan reference describes a cryptosystem that facilitates distribution of session keys through a central intermediary using split private key public encryption. Ganesan describes generating a first and second user private encryption key and a corresponding first and second user public encryption key for a respective first and second user of a split key public cryptosystem. The private encryption keys are divided into first and second user key portions and corresponding first and second central authority key portions. The first and second user key portions are respectively disclosed to the first and second users. The central authority key portions and the public encryption keys are disclosed to a central authority. When the first user requests to establish a communications session with the second user, the central authority generates **a first encrypted session key** using the first central authority key portion and corresponding

public encryption key, and **a second encrypted session key** using the second central authority key portion and corresponding public encryption key. Ganesan teaches that the first encrypted session key is disclosed to the first user, and the second encrypted session key is disclosed to the second user. Thus, Ganesan teaches that **the first user and the second user receive different session keys**.

In contrast, the presently claimed invention, as recited in independent claims 1, 6, 7, and 15, describes a method and system for "establishing a secure communication channel in an IP telephony network ... wherein communications between the first telephony adapter and the second telephony adapter are **routed through** the first gateway controller and the second gateway controller." A first user is coupled to a first telephony adapter, which is coupled to a first gateway controller. Similarly, a second user is coupled to a second telephony adapter, which is coupled to a second gateway controller. The first gateway controller and the second gateway controller connect to and control user access to the IP telephony network. The path of the communications between the first user and the second user is from the first telephony adapter, then to the first gateway controller, then to the IP telephony network, then to the second gateway controller, and then to the second telephony adapter. Thus, in the presently claimed invention, the communications path from the first telephony adapter to the second telephony adapter is **routed through the first and second gateway controller**, not direct from the first telephony adapter to the second telephony adapter as Barkan teaches.

In further contrast, the presently claimed invention, as recited in independent claims 1, 6, 7, 11, and 15, describes "generating a secret key at the first gateway controller" and "distributing the secret key to the first and second telephony adapters". Thus, **the first telephony adapter and the second telephony adapter receive the same secret key**, not a **different** session key as Ganesan teaches.

The Barkan and Ganesan references, taken either alone or in combination, do not describe a communications path from the first telephony adapter to the second telephony adapter that is routed through the first and second gateway controllers. The communications path described in Barkan utilizes a wired or wireless communication means on the standard communication channel (element 213) as a direct connection between the first user's encryption machine (facility 1) and the second user's encryption

machine (facility 3). Ganesan does not make up for this additional shortcoming of Barkan because it does not describe a communication path from the first telephony adapter to the second telephony adapter that is routed through the first and second gateway controllers as described in the claims.

Furthermore, the Barkan and Ganesan references, taken either alone or in combination, do not describe generating a secret key at the first gateway controller, distributing the secret key to the first and second telephony adapters over previously established secure connections, and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key. The first encrypted session key and the second encrypted session key described in Ganesan are **different keys**. Thus, Ganesan does not make up for the shortcomings of Barkan because it does not describe generating a secret key at the first gateway, distributing the secret key to both telephony adapters, and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key as described in the claims.

Since Ganesan fails to supply features missing from Barkan, the combination of Barkan and Ganesan cannot suggest the presently claimed invention and cannot render the claims obvious. Thus, no matter how Barkan and Ganesan may be combined (even assuming, *arguendo*, that one of ordinary skill in the art would be led to combine them) the resulting combination is not the invention recited in independent claims 1, 6, 7, 11, and 15.

Furthermore, the Ganesan reference **teaches away** from the presently claimed invention. The final Office Action fails to address this argument. A person of ordinary skill in the art considering the Ganesan reference in view of the Barkan reference would generate a different secret key for each telephony adapter, and distribute each secret key to the appropriate telephony adapter. Thus, the Ganesan reference teaches away from the presently claimed invention of generating a secret key at the first gateway controller and distributing the secret key to the first and second telephony adapters. Based on the disclosure in Ganesan the person of ordinary skill in the art would be discouraged from generating the encryption key at the gateway, and would be further discouraged from using a separate gateway coupled to the first and second telephony adapter that is then

coupled to the first and second user. Thus, a *prima facie* conclusion of obviousness cannot be drawn from the combination of the Barkan and Ganesan references. Applicants respectfully submit that Ganesan fails to provide a basis for a rejection under 35 U.S.C. § 103, at least because Ganesan teaches away from generating a secret key at the first gateway controller and distributing the secret key to the first and second telephony adapters. Because Ganesan is an improper basis for rejecting Applicants' claims, the combination of Ganesan with Barkan, or with other prior art references, also is an improper basis for rejecting Applicants' claims.

For at least the aforementioned reasons, independent claims 1, 6, 7, 11, and 15 are patentable over the Barkan and Ganesan references, either taken alone or in combination. Thus, the Examiner should withdraw the 35 U.S.C. § 103 obviousness rejection as to independent claims 1, 6, 7, 11, and 15.

Claims 2-5, 8-10, 12-14, and 16-19 depend from either independent claim 1, 6, 7, 11, or 15. For the previously stated reasons, independent claims 1, 6, 7, 11, and 15 are allowable. Since any claim that depends from an allowable independent claim is also allowable, the Applicants respectfully submit that the Examiner should also withdraw this rejection as to dependent claims 2-5, 8-10, 12-14, and 16-19.

Claims not specifically mentioned above are allowable due to their dependence on an allowable base claim. In light of the arguments presented above, it is respectfully submitted that all pending claims are in condition for allowance. Reconsideration and withdrawal of the final rejection of the claimed invention is respectfully requested.

Respectfully submitted,
ALEXANDER MEDVINSKY, et al.

Date: April 27, 2009

BY: /Stewart M. Wiener/
Stewart M. Wiener
Registration No. 46,201
*Attorney for Applicants*

MOTOROLA, INC.
101 Tournament Drive
Horsham, PA 19044
Telephone: (215) 323-1811
Fax: (215) 323-1300